I. General Remarks Concerning This Response

Claims 1-25 are currently pending in the present application. No claims have been amended, added, or canceled. Reconsideration of the claims is requested.

II. Summary of Present Invention

A method and system are presented for processing signed applets that are distributed over the Internet. Using the described framework, an applet that is packaged as a Netscape-signed or JDK-signed jar file or as an Internet Explorer-signed cab file is processed within the same Java runtime environment, irrespective of the browser type, such as Netscape Navigator, Internet Explorer, or JDK, that is used to execute the applet. When the applet is executed, the framework verifies one or more applet signatures using the same algorithm that was used to sign the applet, verifies the signer(s) of the applet, and stores information about the signers so that they can be honored by a security policy when permissions for the applet are determined. According to another aspect of the invention, a method for executing a signed applet packaged in a given file, e.g., a jar file or a cab file, includes a number of process steps. Upon loading a given class, the process begins by determining whether a signer in the given file applies the class. If so, a verification routine is executed to verify the signer that generated the signature. Following a successful verification, the method continues by determining whether the signer is identified in a policy entry. If so, the routine populates a permission set for the class by awarding the class a given permission as specified in the policy entry. When the applet makes an initial request that requires the permission, the permission set of the class is then used to determine whether the class has the requisite permissions.

III. 35 U.S.C. § 102(b)–Anticipation–*Devine et al.*

The Office action has rejected claims 1-25 under 35 U.S.C. § 102(b) as anticipated by Devine et al., "Secure customer interface for web based data management", U.S. Patent No. 6,598,167 B2, filed 09/26/1997, issued 07/22/2003. This rejection is respectfully traversed.

The rejection of independent claim 1 states in its entirety:

> As per claim 1; A method for executing a signed applet packaged in a given file [col. 2, lines 55-col. 3, line 8, col. 5, lines 57-col. 6, line 3], comprising: upon loading a class, determining whether a signature in the given file type applies to the class [col. 6, lines 13-33, 39-62, col. 14, lines 53-col. 16, line 33, figure 7 and accompanying description; if so, executing a verification procedure to verify the signature and the identity of a signer that generated the signature [col. 8, lines 31-60, col. 12, lines 16-col. 14, line 39]; following a successful verification, determining whether the signer is identified in a policy entry [col. 16, lines 47-56]; and if the signer is identified in the policy entry, populating a permission set for the class [col. 16, lines 47-col. 17, line 8].

As is apparent from the copy of the rejection that is included hereinabove, the rejection does not provide any detail or any argument as to which specific elements of the system that is disclosed in Devine et al. correspond to the claimed elements of the present application. The rejection merely points to large portions of text within Devine et al. for the claim elements. Applicant notes that the lack of explanatory detail in the rejection with respect to individual claim elements obfuscates the extent to which the disclosure in Devine et al. may or may not disclose some of the claimed features. In other words, the rejection points to entire sections of Devine et al. rather than comparing specific features of Devine et al. against specific claim elements through the use of specific analogies that could be discussed and critiqued by Applicant. Thus, the rejection obfuscates the issue of anticipation by making broad references to sections of Devine et al. without providing any guidance on

the manner in which one is to interpret Devine et al. as anticipating the claimed invention of the present application.

More importantly, though, Applicant asserts that Devine et al. fails to disclose some of the elements of claim 1, notwithstanding the references from the rejection into portions of Devine et al. that supposedly disclose these claim elements. Independent claim 1 reads:

> 1. A method for executing a signed applet packaged in a given file, comprising:
>
> upon loading a class, determining whether a signature in the given file type applies to the class;
>
> if so, executing a verification procedure to verify the signature and the identity of a signer that generated the signature;
>
> following a successful verification, determining whether the signer is identified in a policy entry; and
>
> if the signer is identified in the policy entry, populating a permission set for the class.

Specifically, the rejection states that Devine et al. discloses the third element of claim 1, i.e. "following a successful verification, determining whether the signer is identified in a policy entry". As recited earlier in claim 1, the signer has generated a signature for a signed applet that has been packaged in a file, e.g., a JAR file or a CAB file. When the third element is considered in the context of the entire claim, the third element recites that the signer of the verified signature on the applet is determined to be identified in a policy entry. It is not the case that the third element recites that any signer is identified in a policy entry. However, the rejection incorrectly argues that the third element of claim 1 is disclosed in Devine et al. by making reference to a portion of Devine et al. that discusses a user and user entitlements. The user and

the signer are not equivalent; moreover, the user entitlements are not equivalent to the signer's permissions in a policy entry.

In particular, the rejection states that Devine et al. discloses the third element of claim 1, i.e. "following a successful verification, determining whether the signer is identified in a policy entry", is disclosed in the following text at column 16, lines 47-56 (emphasis added):

> Referring again to FIG. 10, the backplane communicates with the StarOE server 49 to retrieve **the user's entitlements** in step 308. **The entitlements represent specific services the user has subscribed and has privilege to access.** It also describes what entitlements the user may have within any single service. For example, from the COUser context, the backplane can obtain the list of applications that the user is entitled to access. In addition, each COApp holds a set of entitlements within that application in COAppEntitlements object.

The user to which this portion of Devine et al. is referring is described previously in Devine et al., e.g., in the text at column 16, lines 17-29 (emphasis added):

> Referring back to FIG. 10, once the browser type has been confirmed, the logon applet checks for the name/password entry and instantiates a session object in step 292, communicating the name/password pair to the enterprise system. **The session object sends a message containing the name/password to the StarOE server 49 for user validation** in step 294.
>
> **When the user is properly authenticated by the server** in step 296, another Web page which launches the backplane object is downloaded in steps 298, 300, 304. This page is referred to as a home page. At the same time, all the remaining application software objects are downloaded in CAB or JAR files as indicated at step 302.

As should be apparent, the user is the user of the browser application. The system in Devine et al. verifies the identity of the user of the browser application and then determines the entitlements of that user with respect to subscribed services. As mentioned above, the user and the signer are not equivalent; the user entitlements are not equivalent to the signer's

permissions in a policy entry. The present invention discloses that the requests from a class within an executing applet (e.g., within a browser application) are granted or denied based on the permissions for the signer of the signed applet; Devine et al. discloses that requests for subscribed services are granted or denied based on the entitlements of the user of the browser application that is executing an applet, which is quite different from the present invention. Therefore, contrary to the argument in the rejection, Devine et al. does not disclose the third element of claim 1.

Given that Devine et al. does not disclose the third element of claim 1, i.e. "following a successful verification, determining whether the signer is identified in a policy entry", it is not possible for Devine et al. to disclose the fourth element of claim 1, i.e. "if the signer is identified in the policy entry, populating a permission set for the class", because Devine et al. does not disclose the identification of the signer of the signed applet within a policy entry.

Independent claim 11 is another method claim that is similar to independent claim 1; claim 11 differs from claim 1 by including an addition fifth claim element, which recites the feature of "responsive to a request that requires a permission, using the permission set for the class to determine whether the class has the permission." Applicant asserts that the rejection of claim 11 continues the misinterpretation of Devine et al.. Even though Devine et al. may disclose a processing step of providing access to a service for a user based on the user's entitlements, the disclosure of Devine et al. is not equivalent to the fifth element of claim 11 because, in the present invention, the requests are granted or denied based on the permissions for the signer of the signed applet.

Independent claims 1 and 11 are directed to a method; claim 17 is directed to a computer program product; and claim 22 is directed to a system. The Office action uses an anticipation argument against claims 17 and 22 by relying the argument that is used against claim 1. Applicant's arguments with respect to the rejection of claim 1 are similarly applicable against the rejection of claims 17 and 22.

With respect to the dependent claims of independent claims 1, 11, 17, and 22, Devine et al. does not disclose, at a minimum, the subject matter in the independent claims from which these dependent claims depend. Thus, Devine et al. also fails to disclose the features of the dependent claims because these dependent claims include the features of the independent claims.

In fact, most of the rejections of the dependent claims are as non-specific as the rejections of the independent claims from which they depend. Again, the lack of detail in the rejections mirror the lack of disclosure in Devine et al.. For example, dependent claim 5 contains two elements. The first element of claim 5 reads: "determining whether the applet has made a request that requires permission". The second element of claim 5 reads: "if so, using the permission set of the class to determine whether the class has the permission". The rejection of claim 5 cites five portions of Devine et al. containing over two columns of text, yet the rejection does not particular point to any teachings of the claimed features. Some of these portions of Devine et al. appear to have been selected at random because there is no argument as why these portions of Devine et al. seem to be relevant in any manner whatsoever. Applicant asserts that it is not possible to be more specific in the rejection because the reference that is applied against claim 5, i.e. Devine et al., does not disclose the claimed features.

More importantly, the dependent claims recite additional elements, and these elements fail to be disclosed in Devine et

al.. Again, Applicant asserts that the rejections of the dependent claims continue the misinterpretation of Devine et al. that was argued in the rejection of independent claims 1 and 11. Some of the dependent claims merely recite a feature concerning the signature algorithm that may be used within the claimed process. However, most of the dependent claims contain some feature relating to the permission set for the applet as determined from the signer of the signed applet, and Devine et al. fails to disclose these claimed features. For example, it is not possible for Devine et al. to teach the feature of "using the permission set of the class to determine whether the class has the permission", as recited in dependent claim 5, because the system of Devine et al. checks user entitlements, not class permissions that are based on the permission set of a signed applet. The features in the dependent claims are clearly absent from Devine et al., notwithstanding the argument in the rejections.

Devine et al. clearly does not disclose features as required by the language of the claims of the present application. As stated at MPEP § 2131: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Hence, Devine et al. cannot be used as an anticipatory reference, and the rejection of claims 1-25 has been overcome, whereby Applicant requests the withdrawal of the rejection.

IV. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: August 27, 2004

Respectfully submitted,

Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz